English Translation Attached

DERWENT-ACC-NO: 1981-E4288D
DERWENT-WEEK: 198120

TITLE: Security coding system for documents - has cover coding printed on document and optically scanned for comparison with normal text

INVENTOR: SZEPANSKI, W

PATENT-ASSIGNEE: SZEPANSKI W[SZEPI]

PRIORITY-DATA: 1979DE-2943436 (October 26, 1979)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
DE 2943436 A	May 7, 1981	N/A	000	N/A

INT-CL (IPC): B41M003/14; B44F001/12 ; G06K019/06 ; G07C009/00 ; G07D007/00

ABSTRACTED-PUB-NO: DE 2943436A
BASIC-ABSTRACT: The falsification of information printed on documents, identify cards, banknotes etc., is discouraged by additional printing or forming of a coded information pattern.

Typically, the visual information (2) is printed in alpha-numeric form and the coded information is overprinted in the form of square segment patterns (3). An alternative uses a thin plastic film that bonded to the surface of the document under the application of heat. An optical scanning system is used to read the coding pattern and a processor to effect an interpretation routine.

TITLE-TERMS:
SECURE CODE SYSTEM DOCUMENT COVER CODE PRINT DOCUMENT OPTICAL SCAN COMPARE NORMAL TEXT

DERWENT-CLASS: P75 P78 T04 T05

EPI-CODES: T04-C; T05-D; T05-J;

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(11) **DE 29 43 436 A1**

(51) Int. Cl. ³:
G 06 K 19/06
G 07 C 9/00
G 07 D 7/00
B 44 F 1/12
B 41 M 3/14

(21) Aktenzeichen: P 29 43 436.4-53
(22) Anmeldetag: 26. 10. 79
(43) Offenlegungstag: 7. 5. 81

(71) Anmelder:
Szepanski, Wolfram, Dr.-Ing., 5100 Aachen, DE

(72) Erfinder:
gleich Anmelder

(54) Maschinell prüfbares Schutzmuster für Dokumente und Verfahren zur Erzeugung und Prüfung des Schutzmusters

DE 29 43 436 A1

DE 29 43 436 A1

2943436

Patentansprüche

1. Druckfähiges Schutzmuster zum Fälschungsschutz von Dokumenten, das sowohl eine visuelle als auch eine maschinelle Echtheitsprüfung erlaubt, dadurch gekennzeichnet, daß eine flächig verspreizte Echtheitsinformation im Schutzmuster enthalten ist.

2. Schutzmuster nach Anspruch 1., dadurch gekennzeichnet, daß die Echtheitsinformation aus einem kodierten alfanumerischen Text besteht.

3. Schutzmuster nach Anspruch 2., dadurch gekennzeichnet, daß der alfanumerische Text ganz oder teilweise aus dem individuellen Informationen (2) besteht, durch die sich zwei Dokumente gleicher Art unterscheiden.

4. Schutzmuster nach einem der Ansprüche 2. und 3., dadurch gekennzeichnet, daß der alfanumerische Text binär kodiert ist.

5. Schutzmuster nach einem der Ansprüche 1. bis 4., dadurch gekennzeichnet, daß die Verspreizung der Echtheitsinformation durch aneinandergefügte Flächenmuster (3) geschieht, die sich in ihren optischen Eigenschaften im Bereich des sichtbaren und / oder unsichtbaren Lichts unterscheiden.

6. Schutzmuster nach einem der Ansprüche 1. bis 5., dadurch gekennzeichnet, daß es aus unterschiedlichen zueinander orthogonalen oder bipolaren Flächenmustern (3), insbesondere Walsh-Karhunen-Loève Basisfunktionen zusammengesetzt ist.

7. Schutzmuster nach einem der Ansprüche 1. bis 6., dadurch gekennzeichnet, daß es sich auf einer transparenten Kunststoffolie befindet, die mit aggressivem Klebstoff unter Druck und Hitze auf die zu schützenden Oberflächen des Dokuments gebracht wird.

8. Schutzmuster nach einem der Ansprüche 1. bis 6., dadurch gekennzeichnet, daß es direkt auf das zu schützende Dokument gedruckt wird.

9. Schutzmuster nach Anspruch 8., dadurch gekennzeichnet, daß das zu schützende Dokument eine Banknote, ein Scheck oder ein Wertpapier ist.

10. Schutzmuster nach Anspruch 7. und 8., dadurch gekennzeichnet, daß das zu schützende Dokument ein Paßbild oder ein Ausweis ist.

11. Verfahren zur Echtheitsprüfung des Schutzmusters nach einem der Ansprüche 1. bis 10. mit Hilfe der Korrelationsdetektion, dadurch gekennzeichnet, daß die Korrelation mit einem Digitalrechner ausgeführt wird.

12. Verfahren zur Echtheitsprüfung des Schutzmusters nach einem der Ansprüche 1. bis 10., dadurch gekennzeichnet, daß eine Anordnung zur optischen Korrelation benutzt wird.

13. Verfahren zur Erzeugung eines Schutzmusters nach einem der Ansprüche 1. bis 10. dadurch gekennzeichnet, daß ein Digitalrechner benutzt wird, um das Schutzmuster auf das Dokument anzupassen und das Dokument selbst oder eine Druckmatrize hierfür herzustellen.

2943436

Dr.-Ing. Wolfram Szepanski
Harbachtalstraße 21
5100 Aachen

Maschinell prüfbares Schutzmuster für Dokumente und Verfahren zur Erzeugung und Prüfung des Schutzmusters

Die Erfindung bezieht sich auf ein maschinell prüfbares Schutzmuster für Dokumente, das eine über die Fläche des Dokuments verspreizte Echtheitsinformation enthält, sowie auf Verfahren zur Erzeugung des Schutzmusters und zu seiner Echtheitsprüfung.

Unter dem Begriff "Dokument" sollen hier Pässe, Identitätskarten, Berechtigungsausweise, Kreditkarten, Schecks, Banknoten, Wertpapiere und dgl. verstanden werden. Aufgrund der weiten Verbreitung dieser Dokumente und der mit ihnen verbundenen Werte wurden bereits verschiedene Maßnahmen zum Schutz vor Nachahmungen, Radierungen und sonstigen Verfälschungen angewendet. Als besonders sicher können Dokumente gelten, deren Echtheitsmerkmale nur schwer kopierbar oder verfälschbar sind und deren Unverfälschtheit auf verschiedene, von einander unabhängige Weisen und mit geringem Aufwand geprüft werden können. Dabei sollte der Fälschungsschutz vorzugsweise eine einfache visuelle Echtheitsprüfung erlauben, er sollte jedoch auch für eine maschinelle Prüfung durch automatische Lesegräte geeignet sein, um eine zweite, von der visuellen Prüfung unabhängige Kontrolle zu ermöglichen. Darüberhinaus eignen sich maschinell prüfbare Dokumente als Zahlungsmittel für Verkaufs- oder Geldwechselautomaten, als Ausweise für automatische Zugangskontrollen usw. und überall dort, wo eine große Anzahl von Dokumenten wie z. B. Banknoten oder Schecks maschinell registriert, sortiert oder gezählt werden muß. Gegenstand der Erfindung sind deshalb ebenfalls ein Verfahren zur Herstellung von geschützten Dokumenten sowie Verfahren zu ihrer maschinellen Echtheitsprüfung.

Um Nachahmungen zu erschweren und Fälschungen leicht kenntlich zu machen, werden Dokumente vielfach mit einem Schutzmuster überzogen. Am häufigsten verwendet werden komplizierte Linienmuster (Guillochen), die zwar eine visuelle Echtheitsprüfung erlauben, die aber in der Regel nicht maschinell lesbar sind. Dasselbe gilt für Schutzmuster mit einer dreidimensionalen optischen Wirkung, für die in den Auslege- und Offenlegungsschriften (DE-AS 23 34 702 bzw. DT-OS 26 03 558) keinerlei Hinweise auf eine maschinelle Prüfbarkeit gegeben werden.

Weiter sind Verfahren zum Dokumentenschutz bekannt, die auf dem Grundgedanken basieren, daß bestimmte maschinell lesbare Informationen oder Markierungen für einen Fälscher unsichtbar auf einem Dokument angebracht oder in ihm verborgen sind. Dies kann zum Beispiel durch die Verwendung von Materialien mit bestimmten elektrischen, magnetischen oder optischen Eigenschaften erzielt werden. Ein derartiger Dokumentenschutz ist nicht ohne Meßgeräte nachweisbar und kann ohne zusätzliche Maßnahmen auch nicht visuell überprüft werden. Wird die Existenz der unsichtbaren Markierung von einem Fälscher aber dennoch erkannt, so besteht die Gefahr einer Fälschung oder Nachahmung.

Es wurde auch ein Radierschutz vorgeschlagen (DT-AS 25 30 905), bei dem das Dokument von einer homogenen, informationslosen Schutzschicht bedeckt ist, die sich in ihren optischen Eigenschaften von der Informationsdruckfarbe und vom Papier unterscheidet und die Radierversuche in einem Lesegerät sichtbar werden läßt. Nicht erfaßt werden durch dieses Verfahren alle die Fälschungen, die ohne Radierungen dadurch zustande kommen, daß z. B. im Klartext auf das Dokument geschriebene Namensangaben oder Zahlenwerte durch Hinzufügen von Buchstaben oder Ziffern verändert werden.

Es ist ferner bekannt, sehr fälschungssichere Dokumente dadurch zu erzeugen, daß man eine Echtheitsinformation in Form eines Hologramms (DT-AS 25 01 604 und DT-AS 25 46 007) oder eines in Kunststoff eingeprägten, optischen Beugungsgitters (DT-AS 25 55 214) auf einem Dokument anbringt. Ein schwieriges, ungelöstes Problem

ist dabei die Erzeugung von kratz-, knick- und knitterfesten Hologrammen für Schecks und Banknoten, die gleichzeitig dünn, hochflexibel und dauerhaft abnutzungsfest sein müssen. Da die bekannten holographisch gesicherten Dokumente entweder ganz oder wenigstens an ihrer Oberfläche aus Kunststoff bestehen, können außerdem Schwierigkeiten entstehen, wenn die Dokumente nachträglich beschriftet oder gestempelt werden sollen. Bei der Massenherstellung von Dokumenten wirken sich die hohen Herstellungskosten für Hologramme zusätzlich nachteilig aus.

Aufgrund der genannten Mängel sind die bisher bekannten Verfahren des Dokumentenschutzes für bestimmte Arten von Dokumenten entweder garnicht oder nicht ökonomisch anwendbar oder sie erfüllen ihre Schutzfunktion nur unzureichend. Aufgabe der vorliegenden Erfindung ist es deshalb, einen maschinell prüfbaren Fälschungsschutz für Dokumente anzugeben, der in einer bevorzugten Ausführung auch eine visuelle Echtheitsprüfung erlaubt, und der bei allen eingangs definierten Dokumenten anwendbar ist, ohne die genannten Nachteile bisher bekannter Schutzmethoden zu besitzen. Es ist ferner Aufgabe der Erfindung, Verfahren anzugeben, mit denen die Herstellung des Schutzes sowie seine maschinelle Prüfung möglich ist.

Die Grundidee zur Lösung der Aufgabe besteht darin, die zu schützende Fläche eines Dokumentes untrennbar mit einem Schutzmuster zu versehen, das eine kodierte, über die gesamte zu schützende Fläche verspreizte Echtheitsinformation enthält. Als Echtheitsinformation eignen sich dabei beliebige alfanumerische Texte. Erfindungsgemäß wird die Kodierung der Echtheitsinformation und ihre Verspreizung über die zu schützende Fläche dadurch erreicht, daß die einzelnen alfanumerischen Zeichen zunächst durch die Symbole eines zwei- oder mehrwertigen Kodes ersetzt werden. Dabei ist aus der Nachrichtentechnik bekannt, daß sich mit einem n-stelligen und m-wertigen Kode $N = m^n$ verschiedene Zeichen darstellen lassen. Mit Hilfe eines sechsstelligen Binärkodes lassen sich so zum Beispiel insgesamt $N = 2^6 = 64$ verschiedene Buchstaben, Ziffern und Sonderzeichen kodieren, so daß jedes dieser Zeichen durch $n = 6$ binäre Symbole dargestellt wird. Jedem der m verschiedenen

Kodesymbole wird nun eines von m unterschiedlichen Flächenmustern zugeordnet, die als optische Trägersignale für die entsprechenden Kodesymbole verwendet werden. Jedes alfanumerische Zeichen oder Sonderzeichen kann somit durch n flächig angeordnete Flächenmuster repräsentiert werden. Besteht die im Schutzmuster zu kodierende Echtheitsinformation aus k alfanumerischen Zeichen, so ergibt sich durch systematische Anordnung der einzelnen, die Kodesymbole repräsentierenden Flächenmuster ein zusammenhängendes Schutzmuster, das aus insgesamt k · n Flächenmustern aufgebaut ist.

Dem Erfindungsgedanken folgend wird nun vorgeschlagen, dieses Schutzmuster dem zu schützenden Dokument zu überlagern und es mit ihm auf geeignete Weise untrennbar zu verbinden. Die Helligkeitswerte von Dokument und Schutzmuster verbinden sich dabei zu einem optischen Gesamteindruck, der dem der bekannten Linienmuster ähnlich ist. Bei einer visuellen Prüfung auf Unverfälschtheit werden Manipulationen des Dokuments an Verletzungen des Schutzmusters und am veränderten optischen Gesamteindruck erkannt. Da das Schutzmuster nur aus wohldefinierten Grundelementen, nämlich den m unterschiedlichen Flächenmustern aufgebaut ist, läßt sich die im Schutzmuster kodierte Echtheitsinformation durch Unterscheidung der einzelnen Flächenmuster maschinell dekodieren. Ein bei einem Fälschungsversuch zerstörtes Flächenmuster führt zwangsläufig zu einer fehlerhaft dekodierten Echtheitsinformation, so daß die Manipulation maschinell selbst dann erkannt wird, wenn der optische Gesamteindruck des Dokuments unverdächtig erscheint.

Einzelheiten und weitere Eigenschaften der Erfindung werden im folgenden anhand der Zeichnungen erläutert.

Es zeigen

Fig. 1 einen Ausschnitt aus einem Dokument ohne erfindungsgemäßes Schutzmuster

Fig. 2 ein Ausführungsbeispiel eines erfindungsgemäßen Schutzmusters

Fig. 3 einen Ausschnitt aus einem Dokument, das durch ein erfindungsgemäßes Schutzmuster geschützt ist.

Fig. 4 - 9 verschiedene Beispiele für die die Kodesymbole repräsentierenden Flächenmuster

Fig. 10 eine Anordnung zur automatischen Echtheitsprüfung

Fig. 11 eine weitere Anordnung zur automatischen Echtheitsprüfung

Fig. 12 eine Anordnung zur Erzeugung von Dokumenten mit erfindungsgemäßem Schutzmuster

Fig. 1 zeigt einen Ausschnitt aus einem Dokument, das mit üblichen Fälschungsschutzmitteln wie Wasserzeichen, Metallfäden und dgl. versehen sein kann. Dabei ist auf einen Dokumententräger 1, der aus Kunststoff bestehen kann, vorzugsweise aber aus Papier bestehen soll, die das Dokument kennzeichnende Information in Form von Schriftzeichen oder sonstigen Markierungen aufgebracht. Diese Information besteht wenigstens zum Teil aus einer individuellen Information 2, die ein bestimmtes Dokument von anderen Dokumenten der gleichen Art unterscheidet, Bei Ausweisen sind dies vor allem die Ausweisnummer, personenbezogene Daten des Ausweisinhabers, sowie Ausgabestelle und Datum. In Fig. 1 besteht die individuelle Information 2 beispielsweise aus Schriftzeichen, die den Namen der Bank, die Konto- und die Scheoknummer bezeichnen. Vor allem diese individuelle Information ist fälschungsgefährdet und sollte vorzugsweise als Teil der Echtheitsinformation in das Schutzmuster einkodiert werden.Dies verhindert eine Fälsohung der individuellen Information durch Hinzufügen von Klartextzeichen, da die Fälschung durch Vergleich mit der dekodierten Information des Schutzmusters erkannt wird.

In Fig. 2 ist ein erfindungsgemäßes Sohutzmuster sohematisch dargestellt. Es besteht beispielsweise aus der wiederholten Anordnung von 4 unterschiedlichen Flächenmustern 3, die die Symbole eines hier vierwertig angenommenen Kodes repräsentieren. Selbstverständlich sind auch beliebige andere Kodierungen inklusive kryptographischer Verschlüsselungen anwendbar. Zur Reduzierung des Aufwands bei der Herstellung und Prüfung des Schutzmusters wird vorzugsweise ein binärer Kode vorgeschlagen.

Die unterschiedlichen Flächenmuster sind in Fig. 2 durch unterschiedliche Schraffierungen gekennzeichnet und dabei so angeordnet, daß sie ein Schutzmuster bilden, das die gesamte zu schützende Dokumentenfläche bedeckt. Zusätzlich zu den Flächenmustern 3 werden Markierungen 4 vorgesehen, die zum Lesen und Dekodieren der im Schutzmuster enthaltenen Echtheitsinformationen benötigt werden.

Fig. 3 zeigt ein erfindungsgemäß geschütztes Dokument 5, bei dem die individuelle Information 2 Bestandteil der Echtheitsinformation ist und in kodierter Form über die Fläche des Schutzmusters verspreist ist. Die untrennbare Verbindung von Dokument und Schutzmuster kann vorzugsweise durch Überdrucken des Dokuments geschehen. Eine andere Art der Verbindung zeigt Fig. 9 als stark vergrößerten Querschnitt durch ein Dokument. Auf einen Dokumententräger 1, auf den eine individuelle Information im Klartext aufgedruckt ist, wird mit Hilfe eines sehr agressiven Klebstoffes 10 eine dünne, transparente Kunststoffolie 9 aufgebracht, die vorher auf ihrer dem Dokument zugewandten Seite mit einem erfindungsgemäßen Schutzmuster bedruckt wurde. Durch Druck und Hitze läßt sich die Kunststoffolie 9 untrennbar mit dem Dokumententräger 1 verbinden.

Die Flächenmuster 3, aus denen das Schutzmuster gebildet wird, bestehen ihrerseits aus mindestens zwei Arten von Rasterelementen 6, 7 mit unterschiedlichen Reflexions- und / oder Transmissions- und / oder Fluoreszenzeigenschaften im sichtbaren und / oder unsichtbaren Teildes Lichtspektrums. So können zum Beispiel in sich mehrfarbige und verschieden strukturierte Flächenmuster erzeugt werden, die sowohl bei einer visuellen als auch bei einer maschinellen Echtheitsprüfung mit optischen Mitteln unterschieden werden können. Um die Sicherheit des Schutzmusters weiter zu vergrößern, lassen sich zusätzlich andere Prüfmethoden anwenden. So können zum Beispiel unterschiedliche Flächenmuster 3, die unterschiedlichen Kodesymbolen entsprechen, durch Zusätze zur Druckfarbe auch magnetisch unterscheidbar gemacht werden. Hierdurch wird eine Nachahmung des Schutzmusters durch einen optischen Kopiervorgang verhindert.

In Fig. 4 bis Fig. 8 sind verschiedene Ausführungsbeispiele für die Flächenmuster 3 dargestellt. Die Begrenzungslinie einzelner Flächenmuster kann dabei beliebig verlaufen, sie kann z. B. quadratisch, rechteckig, sechseckig oder unregelmäßig wie in Fig. 7 sein. Zweckmäßig werden jedoch solche Begrenzungslinien bevorzugt, die ein lückenloses Aneinanderfügen der Flächenmuster ermöglichen. Ebenso sind die Form und Größe der mindestens zwei Arten von unterschiedlichen Rasterelementen 6, 7 beliebig.

Sind die Schriftzeichen, Markierungen und bildlichen Darstellungen eines Dokuments ebenfalls gerastert, so können die Rasterelemente 6, 7 der Flächenmuster 3 auf beliebige Weise mit den Rasterelementen der Schriftzeichen, Markierungen und bildlichen Darstellungen verschachtelt sein, wie dies an einem Beispiel in Fig. 8 gezeigt ist. Die Rasterelemente 6, 7 können aber auch direkt dem Druckbild der Schriftzeichen, Markierungen und bildlichen Darstellungen überlagert werden. Dabei werden die Helligkeitswerte des ursprünglichen Druckbildes verändert. Um Verdeckungen des Druckbildes zu vermeiden, müssen Helligkeitswerte, Größe und Form der Rasterelemente dem zu schützenden Dokument angepaßt werden.

Zur Kodierung der Echtheitsinformation besonders geeignete Flächenmuster 3 sind gewisse, orthogonale Karhunen-Loève Basisfunktionen, die man durch eine Karhunen-Loève Orthogonalzerlegung des zu schützenden Dokuments gewinnt. Die Theorie der Orthogonalzerlegung von Funktionen ist aus der Mathematik bekannt und wird in der Nachrichtentechnik auf Signale angewendet. Einzelheiten zu einer derartigen Anpassung der Flächenmuster 3 an die zu schützenden Dokumente sind in dem Artikel " A Signal Theoretic Method for Creating Forgery Proof Documents for Automatic Verification", Proceedings of Carnahan Conference on Crime Countermeasures, University of Kentucky, Lexington, 16. - 18. Mai 1979, Seite 101 - 109, zu finden.

Die Verwendung von gewissen, schachbrettartigen Karhunen-Loève Basisfunktionen ermöglicht wegen der Orthogonalität der Basisfunktionen einerseits eine optimale Unterscheidbarkeit unterschied-

licher Flächenmuster und gewährleistet eine besonders störunempfindliche Rückgewinnung der im Schutzmuster enthaltenen Echtheitsinformation. Ähnliche Ergebnisse werden durch die Verwendung von schachbrettartigen Walsh-Funktionen als Flächenmuster 3 erzielt.

Fig. 12 stellt eine Anordnung dar, mit der die für ein Dokument optimalen Flächenmuster bestimmt und ein Dokument mit dem erfindungsgemäßen Schutzmuster versehen werden kann. Der Dokumententräger 1 wird zusammen mit der zu schützenden individuellen Information 2 durch ein optisches System 11 und einen opto-elektrischen Wandler 12 z. B. zeilenweise abgetastet. Die den Helligkeitswerten entsprechenden elektrischen Signale werden durch den Analog-Digital-Umsetzer 13 digitalisiert und mit Hilfe des Digitalrechners 14 in orthogonale Karhunen-Loève Basisfunktionen zerlegt. Als geeignete Flächenmuster werden die Basisfunktionen ausgewählt, deren Zerlegungskoeffizienten die geringsten Varianzen besitzen. Eine als alfanumerischer Text über die Tastatur 25 eingegebene Echtheitsinformation wird durch den Digitalrechner 14 nach einem vorgegebenen Kode, z. B. binär, kodiert. Die Kodesymbole der so kodierten Echtheitsinformation werden vom Digitalrechner anschließend durch die ausgewählten Flächenmuster ersetzt und den digital gespeicherten Helligkeitswerten des ursprünglichen Dokuments zusammen mit einer Lesemarkierung 4 überlagert. Nach einer Digital-Analog-Umsetzung kann das erfindungsgemäß geschützte Dokument von einem elektro-optischen Wandler 24 entweder auf einen lichtempfindlichen Dokumententräger oder auf eine Druckmatrize aufgezeichnet werden. Eine mögliche Anwendung für die Anordnung der Fig. 12 liegt beispielsweise darin, ein Paßfoto mit einem Schutzmuster zu überlagern, das die personenbezogenen Daten des Ausweisinhabers in kodierter Form enthält. Ausweisfälschungen durch Austausch des Paßfotos werden so verhindert.

Fig. 10 zeigt eine Anordnung zur Echtheitsprüfung eines Dokumentes 5, das mit einem erfindungsgemäßen Schutzmuster versehen ist. Sie ist bis auf die Tastatur 25 und den elektro-optischen Wandler 24, an dessen Stelle die alfanumerische Anzeige 15 tritt, identisch.

2943436

Die Unterscheidung der den Kodesymbolen entsprechenden Flächenmuster erfolgt im Digitalrechner 14 mit Hilfe der Korrelationsdetektion, einem Verfahren, das aus der Nachrichtentechnik und der Mustererkennung bekannt ist. Hierbei wird die bereits erwähnte Markierung 4 zur Synchronisation des Abtasters verwendet. Nach der Dekodierung wird die im Schutzmuster enthaltene Information in der Anzeige 15 angezeigt. Fälschungen lassen sich durch Vergleich mit dem Klartextaufdruck des Dokuments erkennen.

Fig. 11 zeigt schematisch eine weitere Anordnung zur Echtheitsprüfung eines Dokumentes 5 mit Schutzmuster, die auf dem Prinzip der optischen Korrelation beruht. Zur Vereinfachung der Beschreibung sei angenommen, daß das Schutzmuster binär kodierte Daten enthält, die mit nur einem einzigen Flächenmuster dargestellt sind. Dieses Flächenmuster ist je nach Kodesymbol positiv oder negativ (invertiert)* im Schutzmuster enthalten. Das Dokument 5 befindet sich in der vorderen Brennebene der Linse 17 und wird durch eine kohärente Lichtquelle 16 beleuchtet. In der hinteren Brennebene der Linse 17 und gleichzeitig in der vorderen Brennebene der Linse 19 befindet sich ein Hologramm 18 des datentragenden Flächenmusters. Die in der hinteren Brennebene der Linse 19 auf einer Mattscheibe 21 entstehenden Helligkeitsverteilungen enthalten die Autokorrelation der Flächenmuster mit positiven oder negativen Vorzeichen. Um die binären Kodesymbole am Vorzeichen der Autokorrelation zu unterscheiden, wird die Mattscheibe gleichzeitig durch einen kohärenten Referenzstrahl 20 beleuchtet, der eine Auslöschung derjenigen Helligkeitsverteilungen bewirkt, die negativen Korrelationswerten entsprechen. Die hinter einer Lochblende 22 angebrachten Photodetektoren 23 wandeln die Hell-Dunkel-Verteilung in elektrische Signale, die von einem Analog-Digital-Umsetzer 13 digitalisiert und vom Digitalrechner 14 dekodiert und in der alfanumerischen Anzeige 15 angezeigt werden.

In der Erfindung wird ein neuartiges Schutzmuster angegeben, das einen ähnlichen Schutz vor Fälschung bietet, wie ein Hologramm, das jedoch im Gegensatz zu Hologrammen drucktechnisch auf einem Dokument angebracht werden kann und vielseitiger einsetzbar ist

* oder um 90° gedreht

als Hologramme. Das erfindungsgemäße Schutzmuster erlaubt außerdem eine visuelle Echtheitsprüfung und kann durch zusätzliche Maßnahmen wie magnetisch wirksame Druckfarben vor einer optischen Nachahmung geschützt werden. Es stellt somit eine wesentliche Erweiterung der bisher bekannten Methoden zum Fälschungsschutz von Dokumenten dar.

Nummer: 29 43 436
Int. Cl.³: G 06 K 19/06
Anmeldetag: 26. Oktober 1979
Offenlegungstag: 7. Mai 1981
2943436

NACHGEREICHT

P 29 43 436.4

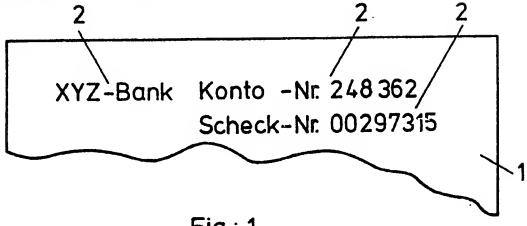

Fig.: 1

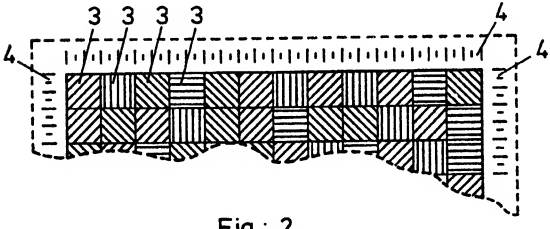

Fig.: 2

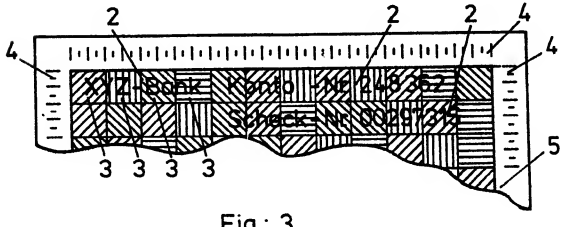

Fig.: 3

NACHGEREICHT

2943436

P 29 43 436.4

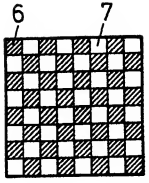

Fig.: 4

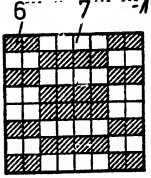

Fig.: 5

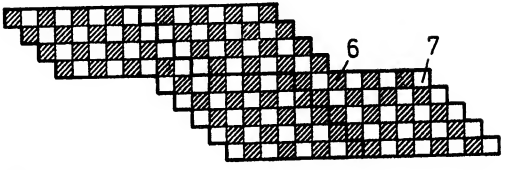

Fig.: 7

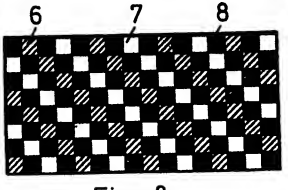

Fig.: 8

Fig.: 6

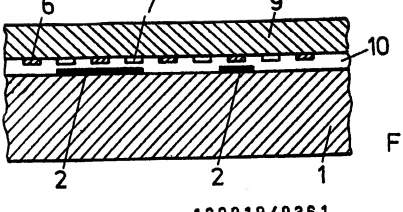

Fig.:9

2943436

P 29 43 436.4

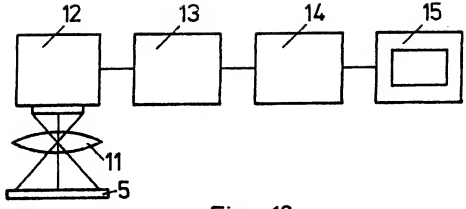

Fig.: 10

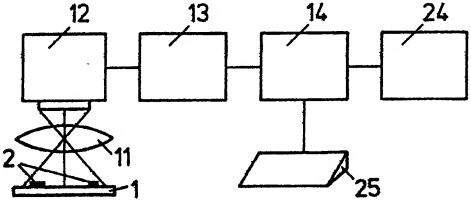

Fig.: 12

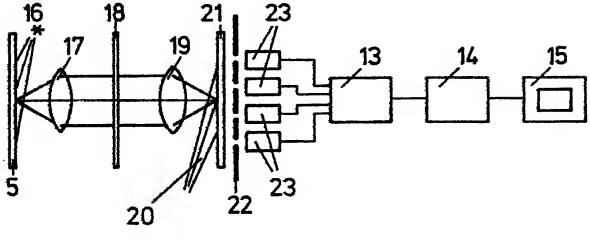

Fig.: 11

PTO 01-525

German Patent No. 29 43 436 A1

MECHANICALLY TESTABLE PROTECTIVE PATTERN FOR DOCUMENTS AND METHOD FOR PRODUCTION AND TESTING OF THE PROTECTIVE PATTERN

Wolfram Szepenski

UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. NOVEMBER 2000
TRANSLATED BY THE RALPH MCELROY TRANSLATION COMPANY

FEDERAL REPUBLIC OF GERMANY
GERMAN PATENT OFFICE
PATENT NO. 29 43 436 A1
(Offenlegungsschrift)

Int. Cl.[3]:	G 06 K 19/06 G 07 C 9/00 G 07 D 7/00 B 44 F 1/12 B 41 M 3/14
Filing No.:	P 29 43 436.4-53
Filing Date:	October 26, 1979
Publication Date:	May 7, 198

MECHANICALLY TESTABLE PROTECTIVE PATTERN FOR DOCUMENTS AND METHOD FOR PRODUCTION AND TESTING OF THE PROTECTIVE PATTERN

Applicant:	Szepenski, Wolfram
Inventor:	Szepenski, Wolfram

Claims /1*

1. Printable protective pattern for forgery protection of documents, which permits both visual and mechanical authentication, characterized by the fact that surface-straddling authentication information is contained in the protective pattern.

2. Protective pattern according to Claim 1, characterized by the fact that the authentication information consists of a coded alphanumeric text.

3. Protective pattern according to Claim 2, characterized by the fact that the alphanumeric text consists fully or partially of the individual information (2), through which two documents of the same type are distinguished.

4. Protective pattern according to one of Claims 2 and 3, characterized by the fact that the alphanumeric text is binary-coded.

* [Numbers in the margin indicate pagination of the original text.]

5. Protective pattern according to one of Claims 1 to 4, characterized by the fact that straddling of the authentication information occurs by surface patterns (3) joined to each other, which differ in their optical properties in the region of visible and/or invisible light.

6. Protective pattern according to one of Claims 1 to 5, characterized by the fact that it is composed of different bipolar surface patterns (3) or surface patterns orthogonal to each other, especially Walsh or Karhunen-Loeve base functions.

7. Protective pattern according to one of Claims 1 to 6, characterized by the fact that it is situated on a transparent plastic film, which is applied under pressure and heat to the surfaces of the document being protected with an aggressive adhesive.

8. Protective pattern according to one of Claims 1 to 6, characterized by the fact that it is /2
printed directly on the document being protected.

9. Protective pattern according to Claim 8, characterized by the fact that the document being protected is a bank note, a check or security.

10. Protective pattern according to Claims 7 and 8, characterized by the fact that the document being protected is a passport or identification.

11. Method for authentication of the protective pattern according to one of Claims 1 to 10 by means of correlation detection, characterized by the fact that the correlation is conducted with a digital computer.

12. Method for authentication of the protective pattern according to one of Claims 1 to 10, characterized by the fact that an arrangement for optical correlation is used.

13. Method for production of a protective pattern according to one of Claims 1 to 10, characterized by the fact that a digital computer is used, in order to adjust the protective pattern to the document, and to produce the document itself or a printing matrix for it.

The invention concerns a mechanically testable protective pattern for documents, which /3
contains authentication information that straddles the surface of the document, as well as a method for production of a protective pattern and its authentication.

The term "document" is understood here to mean passports, identity cards, authorization papers, credit cards, checks, bank notes, securities, etc. Owing to the widespread use of these documents and the value connected with them, various measures to protect against imitation, erasure and other forgery have already been used. Documents whose authentication features are difficult to copy or forge, and whose authenticity can be checked in different ways independent of each other at low cost, are considered particularly secure. The forgery protection should then preferably permit simple visual authentication, but should also be suitable for mechanical testing by automatic readers, in order to permit a second check independent of visual examination. Moreover, mechanically testable documents are suitable as means of payment for vending or money exchanging machines, as identifications for automatic access controls, etc., and anywhere

a large number of documents, like bank notes or checks, must be mechanically recorded, sorted or counted. The object of the invention is therefore also a method for production of protected documents and a method for their mechanical authentication.

To hamper imitation and to make forgery easily recognizable, documents are often coded /4
with a protective pattern. Complicated line patterns (guilloche) are most often used, which do permit visual authentication, but generally are not mechanically readable. The same applies for protective patterns with a three-dimensional optical effect, for which no indications of mechanical testability are mentioned in the Examined and Unexamined Patent Applications (DE-AS 23 34 702 and DT-OS 26 03 558).

Methods for document protection are also known which are based on the fundamental idea that specific mechanically readable information or markings are applied to a document invisible to a forger or are concealed in it. This can be achieved, for example, by using materials with specific electrical, magnetic or optical properties. Such document protection is not detectable without measurement instruments, and also cannot be visually checked without additional means. However, if the existence of the invisible marking is recognized by a forger, the hazard of forgery or imitation exists.

Erase protection has also been proposed (DT-AS 25 30 905), in which the document is covered with a homogeneous protective layer free of information, which differs in its optical properties from the information printing ink and from the paper and reveals attempts at erasure in a reading device. All forgeries that come about without erasure, owing to the fact that alterations are made, for example, in the clear text of name information or numerical values written on the document by addition of letters or numbers, are not detected by this method.

It is also known to produce highly forgery-proof documents by applying authentication information in the form of a hologram (DT-AS 25 01 604 and DT-AS 25 46 007) or an optical diffraction grating embossed in plastic (DT-AS 25 55 214) to a document. A difficult, unsolved problem is then the production of scratch-proof, nonbuckling and crease-proof holograms for /5
checks and bank notes, which must simultaneously be thin, highly flexible and permanently wear-resistant. Since the known holographically secured documents consist either entirely of plastic or consist of plastic on their surface, difficulties can also arise when the documents are to be subsequently written on or stamped. In mass production of documents, the high production costs for holograms are an additional shortcoming.

Because of the mentioned deficiencies, the previously known methods of document protection are either not applicable at all for certain types of documents or are not economical, or they only insufficiently fulfill their protective function. The task of the present invention is therefore to provide mechanically testable forgery protection for documents, which in a preferred variant, also permit visual authentication, and which can be used in all the documents defined at

the outset without having the mentioned drawbacks of previously known protective methods. Another task of the invention is to provide a method with which the production of the protection and its mechanical testing are possible.

The basic idea to solve the task consists of providing the surface of the document being protected with an inseparable protective pattern, which contains coded authentication information that straddles the entire surface being protected. Any alphanumeric text is suitable as authentication information. Coding of the authentication information and the straddling of the surface being protected is achieved according to the invention in that the individual alphanumeric characters are initially replaced by the symbols of a two- or multivalue code. It is known from information technology that $N = m^n$ different characters can be represented with an N-place and m-value code. By means of a six-place binary code, for example, a total of $N = 2^6 = 64$ different letters, numbers and special characters can be coded, so that each of these characters is represented by $n = 6$ binary symbols. One of m different surface patterns is now allocated to each of the m different code symbols, which are used as optical carrier signals for the corresponding code symbols. Each alphanumeric character or special character can therefore be represented by n surface patterns arranged on the surface. If the authentication information to be coded in the protective pattern consists of k alphanumeric characters, a coherent protective pattern constructed from a total of $k \cdot n$ surface patterns is obtained by systematic arrangement of the individual surface patterns representing the code symbols. /6

According to the idea of the invention, it is now proposed to superimpose this protective pattern on the document being protected and attaching it inseparably by appropriate means. The brightness values of the document and protective pattern are then combined to an overall optical impression similar to the known line pattern. During visual examination for authenticity, manipulations of the document are recognized in damage to the protective pattern and the altered optical overall impression. Since the protective pattern is constructed only from well defined base elements, namely, the m different surface patterns, the authenticity information coded in the protective pattern can be mechanically decoded by distinguishing the individual surface patterns. A surface pattern destroyed in an attempt at forgery necessarily leads to incorrectly decoded authenticity information, so that the manipulation is even recognized mechanically when the overall optical impression of the document appears unsuspicious.

Details and additional attributes of the invention are explained below with reference to the drawings.

In the drawings

Figure 1 shows a cutout from a document without the protective pattern according to the invention

Figure 2 shows a practical example of a protective pattern according to the invention

Figure 3 shows a cutout from a document protected by a protective pattern according to the invention

Figures 4-9 show different examples for the surface patterns representing the code symbols /7

Figure 10 shows an arrangement for automatic authentication

Figure 11 shows an additional arrangement for automatic authentication

Figure 12 shows an arrangement to produce documents with the protective pattern according to the invention.

Figure 1 shows a cutout from a document that can be provided with ordinary forgery protective means, like watermarks, metal threads, etc. In this case, the information characterizing the document is applied in the form of written characters or other markings to a document carrier 1, which can consist of plastic, but preferably consists of paper. This information consists at least partly of individual information 2 that distinguishes a specific document from other documents of the same type. In identifications, this information is mostly the identification number, person-related data of the identification holder, as well as issuing office and date. In Figure 1, the individual information 2 consists, for example, of written characters that denote the name of the bank, the account and the check number. It is this individual information above all that is threatened by forgery and should preferably be encoded as part of the authentication information in the protective pattern. This prevents forgery of the individual information by adding clear text characters, since forgery is recognized by comparison with the decoded information of the protective pattern.

A protective pattern according to the invention is schematically depicted in Figure 2. It consists, for example, of the repeated arrangement of 4 different surface patterns 3, which represent the symbols of a code that is assumed to be a four-value code here. Naturally, any other codes, including cryptographic codes, are also usable. To reduce expense in production and examination of the protective pattern, a binary code is preferably proposed.

The different surface patterns are marked in Figure 2 with different shadings and arranged so that they form a protective pattern that covers the entire document surface being protected. In addition to the surface patterns 3, markings 4 are provided, which are necessary for reading and decoding of the authenticity information contained in the protective pattern. /8

Figure 3 shows a protected document 5 according to the invention, in which the individual information 2 is a component of the authenticity information and straddles the surface of the protective pattern in coded form. The inseparable connection of the document and protective pattern can preferably occur by overprinting of the document. Another type of connection is shown in Figure 9 as a strongly enlarged cross section through a document. A thin, transparent plastic film 9, which was printed on its side facing the document with a protective

pattern according to the invention beforehand, is applied to a document carrier 1, on which individual information is printed in clear text by means of a very aggressive adhesive 10. The plastic film 9 can be joined inseparably to the document carrier 1 by pressure and heat.

The surface pattern 3, from which the protective pattern is formed, consists, in turn, of at least two types of grid elements 6, 7 with different reflection and/or transmission and/or fluorescence properties in the visible and/or invisible part of the light spectrum. For example, multicolored and differently structured surface patterns can be produced that can be distinguished by optical means both during visual and mechanical authentication. To further increase the security of the protective pattern, other test methods can additionally be applied. For example, different surface patterns 3, which correspond to different code symbols, can also be made magnetically distinguishable by addition of printing inks. This prevents imitation of the protective pattern by an optical copying process.

Different practical examples for the surface patterns 3 are shown in Figures 4 to 8. The /9
boundary line of individual surface patterns can then run in arbitrary fashion, for example, it can be square, rectangular, hexagonal or irregular, as in Figure 7. However, those boundary lines that permit gapless joining of the protective patterns are expediently preferred. The shape and size of the at least two types of different grid elements 6, 7 are also arbitrary.

If the written characters, markings and images of a document are also indexed, the grid elements 6, 7 of surface pattern 3 can be interlaced arbitrarily with the grid elements of the written characters, markings and images, as shown in the example in Figure 8. The grid elements 6, 7, however, can also be superimposed directly on the printed image of the written characters, markings and images. The brightness values of the original printed image are then altered. To avoid occultations of the printed image, the brightness values, size and shape of the grid elements must be adapted to the document being protected.

Particularly suitable surface patterns 3 for coding of authenticity information are specific orthogonal Karhunen-Loeve base functions obtained by Karhunen-Loeve orthogonal decomposition of the document being protected. The theory of orthogonal decomposition of functions is known from mathematics and is applied to signals in information technology. Details concerning such adaptation of the surface patterns 3 to the documents being protected can be found in the article "A Signal Theoretic Method for Creating Forgery-proof Documents for Automatic Verification", Proceedings of the Carnahan Conference on Crime Countermeasures, University of Kentucky, Lexington, 16-18 May 1979, page 10-109.

The use of specific checkerboard Karhunen-Loeve base functions, because of the orthogonality of the base functions, permits, on the one hand, optimal distinguishability of the different surface patterns and guarantees a particularly disturbance-insensitive recovery of the /10

authenticity information contained in the protective pattern. Similar results are achieved by using checkerboard Walsh functions as surface patterns 3.

Figure 12 shows an arrangement with which the optimal surface patterns for a document can be determined and a document provided with the protective pattern according to the invention. The document carrier 1 is scanned by line, together with the individual information 2 being protected, by an optical system 11 and an optoelectronic transducer 12. The electrical signals corresponding to the brightness values are digitized by analog-digital converter 13 and decomposed to orthogonal Karhunen-Loeve base functions by means of a digital computer 14. Base functions whose decomposition coefficients possess the least variances are chosen as appropriate surface patterns. Authenticity information entered as alphanumeric text via keyboard 25 is coded by the digital computer 14 according to a stipulated code, for example, a binary code. The code symbols of the authenticity information so coded are then replaced by the selected surface pattern and superimposed on the digitally stored brightness values of the original document, together with a reading mark 4. After digital-analog conversion, the protected document according to the invention can be recorded by an electro-optic converter 24 either on a light-sensitive document carrier or on a printing matrix. One possible application for the arrangement of Figure 12, for example, lies in the fact that a passport photo is superimposed with a protective pattern that contains the personal data of the identity holder in coded form. Identification forgeries by replacement of the passport photo are thus prevented.

Figure 10 shows an arrangement for authentication of a document 5 provided with a protective pattern according to the invention. Except for the keyboard 25 and electro-optic converter 24, in whose place the alphanumeric display 15 appears, it is identical. The distinction of the surface pattern corresponding to the code symbols occurs in digital computer 14 by means /11
of correlation detection, a method known from information technology and pattern recognition. In this case, the already mentioned marking 4 is used for synchronization of the scanner. After decoding, the information contained in the protective pattern is displayed in display 15. Forgeries can be recognized by comparison with the clear text printout of the document.

Figure 11 schematically depicts another arrangement for authentication of a document 5 with a protective pattern based on the principle of optical correlation. To simplify the description, it is assumed that the protective pattern contains binary-coded data, which are represented only with a single surface pattern. This surface pattern is contained in the protective pattern according to the code symbol positive or negative (inverted) or rotated by 90°. Document 5 is situated in the front focal plane of lens 17 and is illuminated by a coherent light source 16. A hologram 18 of the data-carrying surface pattern is situated in the rear focal plane of lens 17 and simultaneously in the front focal plane of lens 19. The brightness distributions developing in the rear focal plane of lens 19 on a glass screen 21 contain the autocorrelation of the surface pattern

with positive or negative signs. To distinguish the binary code symbols in the sign of the autocorrelation, the glass screen is simultaneously illuminated by a coherent reference beam 20, which causes extinction of the brightness distributions that correspond to negative correlation values. The photodetectors 23 applied behind a perforated screen 22 convert the light-dark distribution to electrical signals that are digitized by an analog-digital converter 13 and decoded by digital computer 14 and displayed in the alphanumeric display 15.

A novel protective pattern is mentioned in the invention, which offers protection against forgery similar to a hologram, but in contrast to holograms, can be applied by printing to a document and is more versatile than a hologram. The protective pattern according to the /12
invention also permits visual authentication and can be protected by additional expedients, like magnetically active printing inks, from optical imitation. It therefore represents a significant expansion of previously known methods for forgery protection of documents.

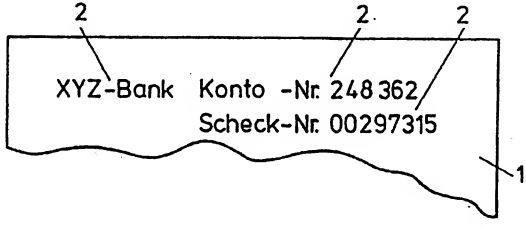

Figure 1

Key: 1 Account No.
2 Check No.

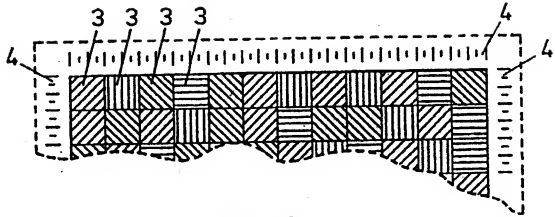

Fig.: 2

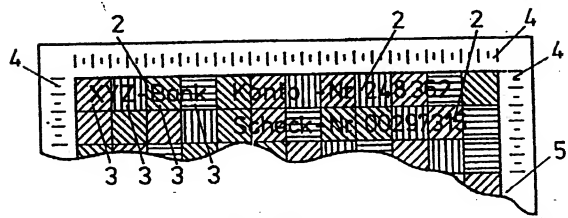

Fig.: 3

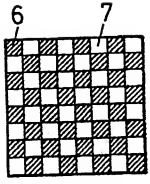

Fig.: 4

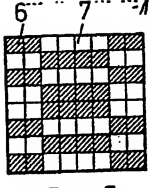

Fig.: 5

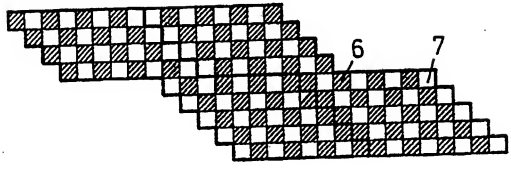

Fig.: 7

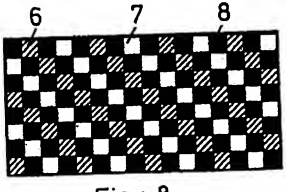

Fig.: 8

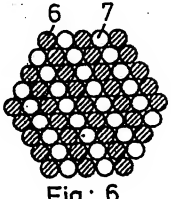

Fig.: 6

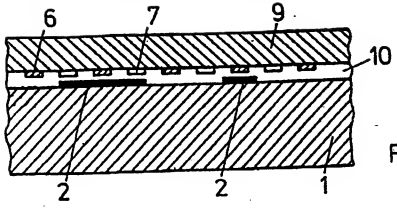

Fig.:9

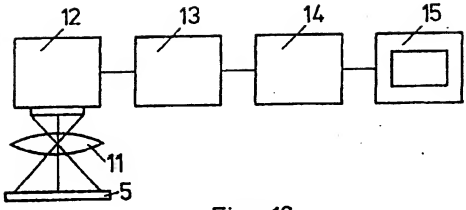

Fig.: 10

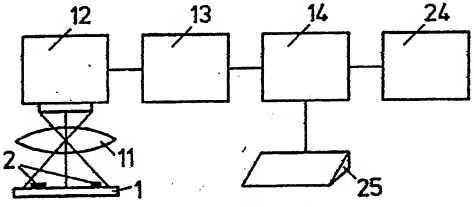

Fig.: 12

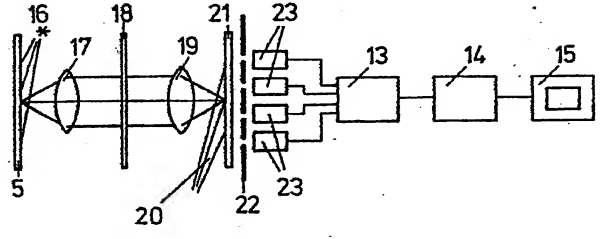

Fig.: 11